PTO/SB/08a (09-06)

Approved for use through 03/31/2007. OMB 0651-0031
S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCI

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Complete if Known bstitute for form 1449A/PTO 10/005,105 Application Number INFORMATION DISCLOSURE Filing Date December 3, 2001 STATEMENT BY APPLICANT First Named Inventor Paul C. Kocher Art Unit 2132 (use as many sheets as necessary) Abdulhakin Nobahar Examiner Name Sheet of 4 44424162-8721 Attorney Docket Number

		t	J.S. PATENT DO	CUMENTS		
Examiner Cite Initials* No.		Document Number Number-Kind Code ² (If known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages o Relevant Figures Appear	
/H.N./	V1	US - 4,202,051	05-06-1980	Davida et al.		
	V2	US - 5,557,346	09-17-1996	Lipner et al.		
	V3	US - 5,623,548	04-22-1997	Aikyama et al.		
	V4	US - 5,625,692	04-29-1997	Herzberg et al.		
	V5	US - 5,625,695	04-29-1997	M'Hraihi et al.		
	V6	US - 5,727,062	03-10-1998	Ritter		
	V7	US - 5,745,577	04-28-1998	Leech		
\neg	V8	US - 5,778,069	07-07-1998	Thomlinson et al.		
	V9	US - 5,870,478	02-09-1999	Kawamura		
	V10	US - 5,982,900	11-09-1999	Ebihara et al.		
1/	V11	US - 5,998,978	12-07-1999	Connell et al.		
$\overline{}$	V12	US - 6,028,454	02-22-2000	Elmasry et al.		
/H.N./	V13	US - 6,345,359	02-05-2002	Bianco		
		1	1			

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No.1	Foreign Patent Number Country Code ³ Number ⁴ Kind Code ³ (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	Ţ¢		
/H.N./	V14	JP 09-163469	06-20-1997	ALPHA Corp.	Only Abstract			
						Ę		
			<u> </u>			L		

Examiner	/Abdulhakim Nobahar/	Date	07/16/2008
Signature		Considered	

*EXAMINER: Initial if reference considered, whether or not clattion is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered, include copy of this form with next communication to applicant. *Applicants roughe distinct soughed ablastic market (opinional). *See Michigania Codes of USPTO Petalet Documents at www.uspia.gov profiles post such decoursed by the two-letter code (MPD Sanadrast 73.). *For Japanese potent comments, the indication of the year of the rignor of the Emperor must precede the serial number of the patent document. *Nind of document by the appropriate symbols as indicated on the document under WIPPO Sanadrast 73.1. *For Japanese potent comments, the indication of the year of the rignor must precede the serial number of the patent document. *Nind of document by the appropriate symbols as indicated on the document under WIPPO Sanadrast 73.1 for possible. *Applicant is to place a defend hand have given a profile to the profile of the profile

This collection of information is required by 37 CFR 1/37 and 158. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentality is governed by 35 USC. 122 and 37 CFR 1/41. This collection is estimated to take 2 hours to complete, including agentaring, preparing, and submitting the complete application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suppleasins for reducing his burden, should be sent to the Chief Information Officer. US. Palent and Trademont Officer. US. Department of Commence, P.O. Box 1450, Alexandria, VA. 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1459, Alexandria, VA. 22313-1450.

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO				cons are required to respond to a collection of into unless it contains a valid UMB control number. Complete if Known				
				Application N	umber	10/005,105		
	INFORMATION DISCLOSURE					December 3, 2001		
STA	STATEMENT BY APPLICANT			First Named In	ventor	Paul C. Kocher		
				Group Art Uni	t :	2132		
(use as many sheets as necessary)			Examiner Nan		Abdulhakin Nobahar			
Sheet				Attorney Dock	et No.	44424162-8721		
		- 0	THER ITEMS - NON F	<u> </u>		IENTS		
Examiner Initials*	CiteNo.	Include na	me of the author (in CAPIT, magazine, journal, serial, s	AL LETTERS), title	of the article (when	n appropriate), title of the	T ²	
/H.N./	V15	INVALIDI	ERNATIONAL SER TY CONTENTION: I. District of Califorr	S, FILED IN C	ASE C04-414	3 JW in US District		
	V16	Electromag on Informa	tion Hiding, Portland	Proceedings of d, Oregon, Apri	the Second In I 1998, pages	ternational Workshop 124-142.		
	V17	Florida: CF	, et al., "CRC Handl RC Press LLC, 1996,	pages 591-634		,		
	V18	CONTENT	VISA INTERNATIONAL SERVICE ASSOCIATION'S FINAL INVALIDITY CONTENTIONS FOR U.S. PATENT NO. 6,278,783 FILED IN CASE C04-4143 JW in US District Court for N. District of California, San Jose Division,					
	V19	ALON, et a	ALON, et al., "Efficient Dynamic-Resharing 'Verifiable Secret Sharing' Against Mobile Adversary", Mar. 25, 1995.					
	V20	CHARNES Verlag, 199	6, et al., "Comments 98.	on Soviet Encr				
	V21	MAURER, UELI M., "A Provably-Secure Strongly-Randomized Cipher", Springer-Verlag, 1998.						
	V22	of paper pr	MEIJER and AKI, "Digital Signature Schemes", May 1982, Extended summary of paper prsented at CRYPTO 81, Santa Barbara, CA, August 1981.					
	V23	November,	SHAMIR, ADI, "How to Share a Secret", Communications of the ACM November, 1979, Volume 22, Number 11.					
/H.N./	/H.N./ V24 VISA INTERNATIONAL SER' CONTENTIONS FOR U.S. PA' 4143 JW in US District Court fo July 16, 2007.				98,442 FILE	D IN CASE C04-		
***************************************	Examiner /Abdulhakim Nobahar/				Date Considered	07/16/2008		

"EXAMINE: Initial ir detends considered, whether or not claid no is in conformance with MEPE PGIS. Draw the through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. 1 Applicant's unique citation designation number (options), 2 see Kinds Codes of USPTIO Patent Documents as www.uspb.goz or MEPE 90.10.4. 2 Enter Office that issued the document, by the wb-their code (WPPO Standard ST.3), 1 For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 4 Kind of document by the appropriate symbols as indicated on the document under WIPPO Standard ST.16 foossible. 4 Foliacinis to piece a check make their Efficients is altabed.

This collection of information is required by 37 CFR 197 and 158. The information is required to obtain or retain a benefit by the public which is o file of and by the USPTO to process) an application. Conferentiating 5 spormed by 58 USC, 122 and 37 CFR 14. This collection is estimated to late 2 younts to complete, including agents, prespiring, and submitting the completed application form to the USPTO. Time will wary depending upon the individual case. Any comments on the amount of time you require into many complete to the complete the form and/or supplections for reducing the buttern, should be sent to the Chief Information Officer, US. Patient and Trademont Cifler, US. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patients, P.O. Box 1450, Alexandria, VA 22313-1450.

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

	Under the Pag	perwork Reduction Act of 1995, no persons are re	quired to respond to a	collection of info uni	ess it contains a valid OMB control	number.	
Substitu	ate for form	1449B/PTO	Complete if Known				
	INFORMATION DISCLOSURE			umber	10/005,105		
STATEMENT BY APPLICANT F			Filing Date		December 3, 2001		
			First Named In	ventor	Paul C. Kocher		
				t	2132 Abdulhakin Nobahar		
(use as many sheets as necessary)			Examiner Nan	ne			
Sheet	3	of 4	Attorney Dock	et No.	44424162-8721		
		OTHER ITEMS - NON F	PATENT LITERA	TURE DOCUM	MENTS		
Examiner Initials*	CiteNo.1	Include name of the author (in CAPIT item (book, magazine, journal, serial, publisher,		etc.), date, page(s		T ²	
/H.N./	V25	BRICKELL, et al., "Fast Expo			ion		
	V26	(Extended Abstract)", Springer DE ROOIJ, PETER, "Efficient					
	V26	Addition Chains", Springer-Ve					
		Cryptology, EUROCRYPT '94		arcprin	t irom Advances in		
\neg	V27	DIMITROV, et al., "An Algor		lar Exponenti	ation", Information		
		Processing Letters, Volume 66					
	V28	DIMITROV, et al., "Two Algo					
		Nonstandard Arithmetics", IEI January 1995.	CE Trans. Fund	damentals, V	ol. E/8-A, No. 1,		
_	V29	GOLLMAN, et al., "Redundar	t Integer Renre	sentations an	d Fast		
		Exponentiation", Designs, Cod					
		Academic Publishers, Boston,					
	V30	HONG, et al., "New Modular I					
- 1		Exponentiation", Springer-Ver EUROCRYPT '96, 1996.	lag, 1998, from	Advances in	Cryptology,		
	V31	JEDWAB and MITCHELL,"	Minimum Wei	tht Modified	Signed-Digit		
		Represenations and Fast Expor					
		Aug. 17, 1989.			· ·		
	V32	KOÇ, ÇETIN K., "High-Radix					
	Exponentiation", Intern. J. Computer Math, v. 40 pp. 139-156, 1991, Gordon and Breach Science Publishers, S.A. (UK).						
	V33	EĞECIOĞLU and KOÇ, "Exp		ng Canonical	Recoding."	 	
V		Theoretical Computer Science	129, pp. 407-4	17, Elsevier,	1994.		
/H.N./	V24 VOC CETINIV Which Sand DSA Implementation BSA Inhomenia						
Examir	ier	/Abdulhakim Nobahar/		Date	07/16/2008		
Signatu	re			Considered	07/10/2008		

"EXAMINE: Initial ir inference considered, whether or not classion is in conformance with NEFP 609. Draw line through classion find in conformance and not considered, include copy of this form with next communication to applicant. "Applicants' number classion designation untimely conformal," See Rivids dodes of UPS s

WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

The record of information is required by 37 CPL 197 and 1.98. The information is required to obtain or reals in a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 38 U.S. 0. 12 and 37 CPL 1.18 collection is estimated to take 2 hours to complete, including gathering, peparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the anomation of time you require to complete inside formation and the complete in the formation of the your require to complete in formation and the complete in the formation of the your plant and Trademank Office, U.S. Department of Commence, P.O. Box 1450, Alexandria, V.A. 2231-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, V.A. 2231-31450.

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO INFORMATION DISCLOSURE STATEMENT BY APPLICANT					Complete if Known			
					Application Number		10/005,105	
					Filing Date		December 3, 2001	
				LICANI	First Named Ir	ventor	Paul C. Kocher	
					Group Art Uni	t	132	
	(use as many sheets as necessary)				Examiner Nam	ie	Abdulhakin Nobahar	
Sheet 4 of 4				4	Attorney Dock	Attorney Docket No. 44424162-8721		
			ОТІ	HER ITEMS - NON F	PATENT LITERA	TURE DOCUM	IENTS	
Examiner Initials*	CiteNo.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.						T ²
/H.N./ V35 LIM and LEE, "More Flexible Exin Cryptology, Springer-Verlag,"								
Examin Signatu		/Abdulh	akim	Nobahar/		Date Considered	07/16/2008	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unque citation designation number (optional). 2 See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. 5 Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to

process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450, DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.